

COMPLIANCE PARTNERS LLP

WWW.COMPLIANCEPARTNERS.NET

1629 K STREET, NW • SUITE 300
WASHINGTON, DC 20006
TEL: (202) 905-0487 • FAX: (202) 449-1388

WRITER'S EMAIL ADDRESS:
AGLENN@COMPLIANCEPARTNERS.NET

March 1, 2010

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

*Re: Annual CPNI Officer Certification
EB Docket No. 06-36*

Dear Ms. Dortch:

On behalf of Latino Communications Corp., and pursuant to 47 C.F.R. § 64.2009(e), attached please find the company's CPNI Officer Certification and Accompanying Statement for calendar year 2009.

Should you have any questions regarding this matter, please do not hesitate to contact the undersigned.

Sincerely,

Audrey Glenn, Esq.
Counsel to Latino Communications Corp.

cc: Best Copy & Printing (via email)

Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2009
EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009.

Date Filed: March 1, 2010

Name of Company: Latino Communications, Corp.

Form 499 Filer ID: 826600

Name of Signatory: Abelardo J. Hoyos

Title of Signatory: Chief Financial Officer

Certification:

I, Abelardo Hoyos, certify that I am the Chief Financial Officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules.

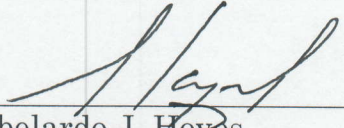
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: _____


Abelardo J. Hoyos
Chief Financial Officer

Accompanying Statement to
Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2009

The policy of Latino Communications, Corp. (hereinafter “Company” or “the Company”) is to protect the confidentiality of CPNI, as required by section 222 of the Telecommunications Act of 1996, and the FCC’s rules promulgated thereunder.

The Company has established operating procedures to ensure compliance with the Commission’s rules governing the protection of CPNI. Specifically, the Company has adopted a *CPNI Compliance Manual*, which is distributed to each employee within the company who either has, or may have, access to CPNI. The key provisions of the Company’s operating procedures and practices with respect to CPNI are set forth below.

I. Use of CPNI:

- The Company does not use, disclose, or permit access to CPNI without customer consent, except as permitted by 47 U.S.C. § 222 and 47 C.F.R. § 64.2005.
- The Company does not use, disclose, or permit access to CPNI for marketing purposes. Nor does the Company disclose or permit access to CPNI to third-parties. Accordingly, the Company has not implemented a system for obtaining customer consent either through the “Opt-in” or “Opt-out” approval processes. Moreover, because the Company does not use, disclose, or permit access to CPNI for any of the foregoing purposes, the Company has no reason to employ customer solicitation notices.

II. Management Safeguards:

- The Company has developed a *CPNI Compliance Manual (Manual)*, which sets forth in detail the FCC’s rules and regulations governing the proper use and disclosure of CPNI. The Manual also sets forth in detail the Company’s internal policies and operating procedures with respect to the protection of CPNI.
- The Company has designated a CPNI Compliance Officer who is responsible for the active monitoring, management, and training of all employees with access to CPNI.
- The company has established a procedure to inform and train all registered employees on the proper use and disclosure of CPNI. Such training includes the distribution of a *CPNI Compliance Manual* to all the registered employees. Each employee must sign a statement verifying that they have received and reviewed the Company’s *CPNI Compliance Manual*, and that they will comply with the Company’s CPNI policies and procedures.
- The Company has established disciplinary procedures for any employee that wrongfully accesses, uses, or discloses CPNI. Any improper use of CPNI is treated as a serious offense, and will result in appropriate disciplinary action.
- Employees are instructed to report each potential CPNI violation or breach to the Company’s CPNI Compliance Officer, and the Company has a process for documenting and investigating each potential violation or breach.

- The Company reviews its CPNI procedures on an ongoing basis to ensure compliance with all FCC regulations, and will revise its procedures as needed to reflect any subsequent revisions to the applicable rules and regulations.

III. Authentication:

- Although the Company is purely a “Carrier’s Carrier” and has no final users as customers, but only wholesale telecommunications companies, the Company uses the procedures specified in 47 C.F.R. § 64.2010 to authenticate a customer’s identity before sharing CPNI with that customer.
- For in-person visits, the Company will disclose CPNI to a customer who first presents a Valid Photo ID matching the Customer’s Account Information.
- The Company will only disclose CPNI over the telephone, based on customer-initiated contact, if the customer first provides the Company with a password that is not prompted by the Company asking for Readily Available Biographical Information or Account Information.
- The Company will permit online access to CPNI through a password that is not prompted by the Company asking Readily Available Biographical Information or Account Information.

IV. Restricted Access to Records

- The Company’s automated information system, which contains the CPNI of the Company’s customers, is password-protected.
- There are very few individuals within the company whose password level is sufficient enough to access the portion of the system containing CPNI. These employees receive specialized training concerning the protection of their passwords and physical workstations to ensure the protection of CPNI.
- All physical facilities containing CPNI are secured, with restricted physical access.

V. Management of Potential CPNI Security Breaches

- Consistent with 47 C.F.R. § 64.2011, the Company has adopted procedures for notifying law enforcement of a breach of its customers’ CPNI.
- The Company will maintain a record of any and all potential CPNI breaches.
- Although the Company has not yet received a request for disclosure of CPNI for purposes of law enforcement, it is the Company’s policy to validate the authenticity of all requests from law enforcement, and ensure that such requests are lawful before releasing CPNI.